UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

19MAG4784

In the Matter of a Warrant for All Content and Other Information Associated with the iCloud Account with Apple IDs [redacted], and [redacted] Maintained at Premises Controlled by Apple, Inc., USAO Reference No. [redacted]

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

[redacted] being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence.

2. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of cellphones in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions,

statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Provider, the Subject Accounts and the Subject Offenses

3. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the iCloud Accounts assigned identification numbers [redacted] (the "Subject Accounts"), maintained and controlled by Apple Inc. ("Apple"), headquartered at 1 Infinite Loop, Cupertino, California 95014. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

4. Based on my review of records obtained from Apple, I have learned the following:

a. The Apple iCloud account assigned identification number [redacted] ("Subject Account-1") is registered to Lev Parnas, using the e-mail address [redacted] (the "Parnas Yahoo E-mail Address"). [1] The Apple iCloud account assigned identification number [redacted] ("Subject Account-2") is also registered to Parnas, using the email address [redacted] (the "Parnas GEP E-mail Address").

b. The Apple iCloud account assigned identification number [redacted] ("Subject Account-3") is registered to Igor Fruman, using telephone numbers [redacted] and e-mail address [redacted] (the "Fruman Google E-mail Address"). I have learned that the telephone number [redacted] was assigned to an iPhone 7 from June 1, 2017 through August

[1] Subject Account-1 was also registered with the telephone number [redacted] which based on my review of telephone records, is subscribed to Parnas's wife, [redacted] However, because his email is associated with Subject Account-1, and for the reasons discussed below, it appears that Lev Parnas is the user of Subject Account-1.

22, 2018, at which time it became assigned to an iPhone 10, and on September 22, 2018, it became assigned to an iPhone XS Max.

c. The Apple iCloud account assigned identification number [redacted] ("Subject Account-4") is registered to [redacted], using telephone numbers [redacted] and [redacted] and the e-mail address [redacted] (the "[redacted] Google E-mail Address"). The telephone number [redacted] was assigned to an iPhone 6S from June 2017 through March 3, 2018, and an iPhone 8 from March 5, 2018 to the present.

5. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of 52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful foreign contributions), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statements in a matter within the jurisdiction of the executive branch), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1346 (honest services fraud), and 18 U.S.C. § 1956 (money laundering) (together, the "Subject Offenses").

C. Services and Records of the Provider

6. Based on my training, experience, and participation in this investigation, as well as my review of publicly-available information, I have learned the following about Apple:

a. Apple designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, a portfolio of consumer and professional software applications, the iOS and Mac OS operating systems, iCloud, and a variety of accessory, service and support offerings. Apple provides email services to its users through email addresses at the domain names mac.com, me.com, and

icloud.com. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and Mac App Store.

b. The iPhone is a line of smartphones designed and marketed by Apple. It runs Apple's iOS mobile operating system. The iPhone has wireless internet capabilities and can connect to many cellular networks around the world. The iPhone can shoot video, send and receive email, browse the Internet, send text messages, provide navigation services via Global Positioning Satellite location technology, record notes, do mathematical calculations, and receive visual and audio voicemail. Apple's text and video messaging application programs are, respectively, iMessage, which enables users of Apple devices to exchange instant messages containing text, photos, videos, locations, and contacts, and FaceTime, which enables those users to conduct video calls. Other functions such as video games, reference works, social networking – including Facebook and Twitter – can be enabled by downloading application programs ("apps" or, singular, "app"). Apple operates an App Store, which offers numerous apps by Apple and third parties.

c. Apple's devices, including iPhones, can be backed up to iCloud, a file hosting, storage, and sharing service provided by Apple. Apple provides users with gigabytes of free electronic storage space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may be used to store iOS device backups, which by default happens automatically for a user of an iCloud account. iCloud accounts may also be used to store or backup data associated with the use of iCloud-connected services including email (iCloud mail), images and video (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud accounts are accessed using an "Apple ID," which is typically created during the setup of an Apple

device or through the registration of an iCloud account. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. Because iCloud accounts are typically linked to iPhones, iCloud accounts are generally registered with a telephone number belonging to an iPhone.

d. Apple maintains the following records and information with respect to iCloud accounts:

i. *Subscriber and billing.* When a user registers an Apple device with an iCloud account, Apple collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and email addresses. Apple also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for some subscribers, Apple maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

ii. *Device information and settings.* Apple maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers for the device, such as the Integrated Circuit Card ID ("ICCID") number, which is the serial number on the device's SIM card, the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's device is captured when iTunes is used on that device to play content associated with an Apple ID. Information about a user's device settings may be captured and stored on the iCloud. Apple also retains records related to communications

between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

iii. *IP records.* Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForget pages on Apple's website.

iv. *Purchase records.* Apple maintains records reflecting a user's app purchases from App Store and iTunes Store.

v. *Address book.* Apple allows subscribers to maintain the equivalent of an address book on the iPhones, comprising telephone numbers, email addresses, and other contact information. That information may be backed up to a user's iCloud account.

vi. *Call history and voicemails*. Apple maintains records reflecting telephone call history and logs for FaceTime calls. That information may be backed up to a user's iCloud account. Apple also allows iCloud subscribers to automatically backup audio and visual voicemails to a subscriber's iCloud account.

vii. *Text message contents.* In general, text messages, Short Message Service ("SMS") messages, Multimedia Messaging Service ("MMS") messages, and iMessages sent to or from a subscriber's account are backed up to the iCloud unless and until the subscriber deletes the messages. If the subscriber does not delete messages, they can remain on the iCloud indefinitely. Even if the subscriber deletes messages off of an electronic device, they may continue to be available on the iCloud for a certain period of time.

viii. *Email contents*. In general, an iCloud account subscriber may elect to store and maintain email content on an iCloud account. When a subscriber makes such an election, any email (which can include attachments such as documents, images, and videos) sent to or from a

subscriber's account, or stored in draft form in the account, is maintained on Apple's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Apple's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Apple's servers for a certain period of time. Additionally, to the extent a subscriber maintains an iCloud Mail account, iCloud enables a user to access Apple-provided email accounts, and email stored in those accounts are maintained by Apple.

ix. *Photos and videos.* In general, an iCloud account subscriber may elect to store and maintain photographs and videos on an iCloud account. When a subscriber makes such an election, any photograph or video stored in the account is maintained on Apple's servers unless and until the subscriber deletes the photograph or video. If the subscriber does not delete the photograph or video, it can remain on Apple's servers indefinitely. Even if the subscriber deletes a photograph or video, it may continue to be available on Apple's servers for a certain period of time. Additionally, to the extent a subscriber uses iCloud Photo Library and My Photo Stream, which can be used to store and manage images and videos, or iCloud Photo Sharing, which allows users to share images and videos with other Apple subscribers, photographs and videos stored in those platforms are also maintained in a subscriber's iCloud account. Apple also retains the metadata – or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data – for photos and videos that are stored on a iCloud account. This metadata includes what is known as exchangeable image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

x. *Documents.* An iCloud account subscriber may elect to store and maintain documents on an iCloud account by saving documents on an iPhone to the iCloud or by using the

service iCloud Drive, which can be used to store documents to the iCloud. Additionally, iWork Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations.

xi. *Web history, search history, and bookmarks.* Apple maintains search and web browsing activity from Safari, Apple's proprietary web browser, as well as bookmarks used to save particular website addresses. iCloud account subscribers may also use iCloud Tabs, which enables iCloud to be used to synchronize webpages opened in Safari web browsers on multiple devices, and iCloud Keychain, which enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

xii. *Third-party application data.* Records and data associated with third-party apps may also be stored on iCloud. For example, the iOS app WhatsApp, an encrypted instant messaging and calling service, can be configured to regularly backup a user's instant messages on iCloud.

xiii. *Location data.* Apple maintains recent location data, collected periodically, from mobile devices. For example, Apple collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. The Apple application Find My iPhone, which allows owners of Apple devices to remotely identify and track the location of devices, allows for location reporting, which allows Apple to periodically store and use a device's most recent location data in connection with an iCloud account.

xiv. *Customer correspondence.* Apple also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's iCloud account.

D. Jurisdiction and Authority to Issue Warrant

7. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

8. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

9. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Prior Applications

10. On or about January 18, 2019, the USAO and FBI sought and obtained from the Honorable Sarah Netburn, Magistrate Judge for the Southern District of New York, a search warrant (the "E-mail Search Warrant") for records in email accounts belonging to Lev Parnas, Igor Fruman, and [redacted], among others, including records associated with the Parnas Yahoo E-mail Address, the Parnas GEP E-mail Address, the Fruman Google E-mail Address, the email address [redacted] (the "Fruman GEP E-mail Address"), the [redacted] Google E-mail Address, and the email address [redacted]

(the "[redacted] GEP E-mail Address"). As discussed below, this affidavit is based in part on my review of responsive materials produced pursuant to the E-mail Search Warrant.

III. Probable Cause Regarding the Subject Offenses

A. Overview of the Scheme

11. The FBI and United States Attorney's Office for the Southern District of New York are investigating political contributions made to campaigns and political action committees by Lev Parnas, Igor Fruman, and Global Energy Producers LLC ("GEP"), but which in fact appear to have been funded by third parties, possibly through foreign sources, in violation of federal law and as a part of the Subject Offenses.

12. The federal campaign finance laws prohibit persons from making contributions in the name of another person. The Federal Election Commission ("FEC") has interpreted the so-called straw donor prohibition as also applying to the creation and use of closely held corporations or corporate LLCs for the purpose of concealing the true source of the funds. The federal campaign finance laws also prohibit foreign nationals from directly or indirectly making political contributions. Additionally, the federal wire fraud statute makes it a crime to defraud political campaigns by depriving them of information about the nature and source of a contribution – specifically, that it is a foreign contribution or a straw donation – necessary for campaigns to exercise their intangible right to control the use of their assets, including how to best allocate the money they raise, while exposing the campaigns to a risk of even greater economic loss, including FEC fines. The federal money laundering statute, as applied here, prohibits the transferring of funds from outside the United States to inside the United States for the purpose of promoting such a wire fraud.

13. Here, there is probable cause to believe that contributions made in the names of Lev Parnas, Igor Fruman, and GEP to various political action committees in connection with the 2018

midterm elections were, in fact, funded by third parties and paid for using money that originated for foreign accounts. In particular, and as described below, it appears that the contributions made in the names of GEP, Parnas, Igor Fruman, and '[redacted] were, in fact, funded by Igor and [redacted] by taking purported "loans" from third parties who funded the loans with wire transfers from foreign bank accounts. As described below, it appears that Parnas, Igor Fruman, and GEP made contributions to the [redacted] PAC, the [redacted] PAC, the [redacted] PAC, the [redacted] PAC, and Congressman [redacted] in violation of the Subject Offenses.

14. To obscure the source of the funds, after receiving the funds from third-party sources, Igor Fruman transferred some of the money to Parnas, who used the money to make contributions in his own name. Additionally, it appears that Parnas and Igor Fruman opened bank accounts in the names of shell entities, including GEP, and moved the foreign funds through those accounts, to conceal the original source of the funds used to make the contributions. Fruman and Parnas also appear to have made false statements to the FEC to obscure their violations of the Subject Offenses. It also appears that Parnas, and later Igor Fruman, became involved in this scheme in order to curry favor with and gain access to politicians. Accordingly, there is probable cause to believe that Fruman, Parnas, and other individuals working for them – including their assistant, [redacted] – have committed the Subject Offenses.

15. As described below, there is probable cause to believe that Parnas, Fruman, and [redacted] used the cellphones linked to the Subject Accounts to, among other things, communicate about these contributions and orchestrate the movement of funds in furtherance of the Subject Offenses. Accordingly, there is reason to believe that evidence of the Subject Offenses will be found on the Subject Accounts.

B. Parnas's Contribution to the [redacted] Fund Using Third-Party Funds

16. In the lead up to the 2016 election, Parnas made a substantial contribution to the [redacted] PAC in his own name, in what appears to be a violation of the Subject Offenses because the funds used to make that contribution came from a third party, who wired the funds to Parnas shortly before the contribution was made, and who had already made a contribution to the [redacted] PAC.

17. Specifically, based on my review of FEC records, financial records, emails obtained pursuant to the E-Mail Search Warrant, public sources, and my training and experience, I have learned the following:

a. On or about October 3, 2016, David Correia, a business partner of Parnas, emailed [redacted] (copying Parnas at the Parnas Yahoo E-mail Address): "It was a great pleasure meeting the other evening . . . I look forward to moving on the Trump dinner and helping to make it a massive success. I already shared with Lev the donation amounts and we will get back to you with details of any/all interested donors." Correia also sent [redacted] "some information about our group [redacted] . . . and a few properties that [redacted] owns." Based on my review of this and other emails, it appears that [redacted] solicited Parnas and Correia to attend a fundraising dinner for Trump, and that in response Correia shared information about investing in the business he and Parnas were operating.

b. On or about October 11, 2016, [redacted] emailed Parnas and Correia a link to a video about Trump, and on or about the same day, he sent Parnas and Correia a registration link for a [redacted] Fund event being held the following day in Hillsboro Beach, Florida. Based on my review of public records, I know that funds contributed to the [redacted] PAC were disbursed to the [redacted] for President, Inc. campaign committee (the "Trump Campaign") and the [redacted] National Committee.

c. On or about October 14, 2016, Correia emailed [redacted] that Parnas had said he and [redacted] had "connected and worked things out." [redacted] indicated on the same day that he had signed an agreement and asked for wire transfer instructions. The agreement signed by [redacted] was an agreement for the investment of $100,000 in a [redacted] fund. Correia then emailed wire transfer instructions for an account at [redacted].

d. Based on my review of bank records, I have learned that on or about October 14, 2016, a bank account in the name of [redacted] LLC, on which Parnas was a signer, received a wire transfer from [redacted] in the amount of $300,000. The reference line on the wire stated "purchase 3 pct Fraud Guarantee LLC," which I understand to be a reference to a purported purchase of three percent of Parnas's business, Fraud Guarantee LLC.

e. On or about October 14, 2016, $100,000 was transferred from the [redacted] account at [redacted] to an account in Lev and [redacted] names at [redacted]. On the same date, $25,000 was wired from the account in Parnas's name to an account in the name of [redacted] which is the name of David Correia's wife.

f. On or about October 24, 2016, Parnas contributed $50,000 to the [redacted] PAC. On the same day, a $5,000 contribution was made in the name of [redacted] to the [redacted] PAC. Based on my review of financial records, it appears that both of the contributions were funded with money from the $300,000 payment by [redacted]

g. [redacted] who is a lawful permanent resident, contributed $15,000 to the [redacted] PAC on October 14, 2016, which was paid as a $2,700 contribution to the Trump Campaign (the maximum) and a $12,300 contribution to the [redacted] National Committee. On or about October 24, 2016, [redacted] again contributed $15,000 to the [redacted] PAC. Because of these contributions, [redacted] was limited in additional contributions he could

make, and accordingly was restricted from making the full contributions made by Parnas and Correia.

18. Based on the foregoing, it appears that the contributions to the [redacted] PAC were solicited and funded by [redacted] but were made in the names of Parnas and [redacted] in violation of the Subject Offenses.

C. Contributions to PACs in 2018 Using Third-Party Funds

19. In 2017 and 2018, Parnas began receiving fundraising solicitations from PACs supporting [redacted] candidates, with a principal focus on the 2018 midterm elections. Some of those solicitations included invitations to meet with Trump and high-ranking congressional representatives. In order attend these events, however, Parnas and his associates were required to make sizeable political contributions. In particular, Parnas and Igor Fruman made sizeable contributions to [redacted] PAC, [redacted] PAC, and [redacted] PAC. It appears, as discussed below, that Parnas and Igor Fruman financed these contributions with funds from third parties, including foreign nationals, in apparent violation of the Subject Offenses.

20. Specifically, based on my review of FEC records, financial records, emails obtained pursuant to the E-Mail Search Warrant, public sources, and my training and experience, I have learned the following:

a. Beginning in or around November 2016, Parnas began receiving email solicitations at the Parnas Yahoo E-mail Address for political contributions. It appears that after receiving those requests for contributions, Parnas attended multiple fundraising events and met congressional representatives and members of the Trump Administration.

b. Based on my review of a newspaper article published in Russian, which has been translated into English, on or about March 3, 2018, Igor Fruman met with Trump at the [redacted]

[redacted] resort in Palm Beach, Florida. The article quotes Fruman, who is pictured with President Trump, as saying: "In the 2016 election, I made donations to Trump's election campaign fund, and now, a year after taking over the presidency, Trump decided it was right again to invite us and turn to his supporters . . . The meeting in [redacted] was the start of his Campaign in the 2020 election . . . And before that, he set the goal of the [redacted] victory in the mid-term elections to Congress in November 2018." Following that meeting, it appears from my review of materials obtained pursuant to the E-mail Search Warrant that Igor Fruman began attending political fundraising events with Parnas.

c. However, in order to attend many of the events, it appears from my review of e-mails obtained pursuant to the E-Mail Search Warrant and public sources that Parnas and/or Fruman were required to make political contributions.

The [redacted] Contribution

21. It appears that one of the contributions that Parnas and Fruman made using third party funds was a $325,000 contribution to the [redacted] PAC. Parnas and Fruman made the contribution to the PAC using the name GEP – rather than their own names – in an apparent effort to obscure their identities and the true source of the funds, in violation of the Subject Offenses.

22. Specifically, based on my review of FEC records, financial records, emails obtained pursuant to the E-Mail Search Warrant, public sources, and my training and experience, I have learned the following:

a. In or about September 2017, Parnas was invited to participate in exclusive events hosted by [redacted], a 501(c)(4) nonprofit entity organized by senior staff members from the Trump Campaign to promote President Trump's policy agenda; [redacted]